FortiClient (Windows) - Release Notes

VERSION 5.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 23, 2017

FortiClient (Windows) 5.6.0 Release Notes

04-560-407213-20171123

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Licensing 6
Standalone Mode 6
Managed Mode 6
Special Notices **8**
Change in SSL VPN default 8
Nested VPN tunnels 8
SSL VPN 98% issues 8
Windows notification of AV being disabled 8
Transition to OS Certificate Store instead of FortiClient's local certificate store 8
Microsoft Windows server support 9
What's New in FortiClient (Windows) 5.6.0 ..... **10**
FortiClient install option 10
Improved FortiClient compliance feature 10
Vulnerability Scan GUI 10
User Avatar retrieval from cloud applications 10
User Avatar sent to FortiAnalyzer 10
Improved remote logging to FortiAnalyzer 10
Sandbox detection 11
New SSL VPN Windows Driver 11
VPN Auto-Reconnect improvement 11
Configurator and Rebranding Tools 11
Installation Information **12**
Firmware images and tools 12
Installation options 13
Upgrading from previous FortiClient versions 13
Downgrading to previous versions 13
Firmware image checksums 13
Product Integration and Support **14**
FortiClient 5.6.0 support 14
Language support 15
Conflicts with third party antivirus products 16

Resolved Issues **17**
Known Issues **20**

Change Log

Date	Change Description
2017-06-15	Initial release of 5.6.0.
2017-06-16	Updated to add support for FortiSandbox 2.4.0.
2017-06-28	Updated to add new, red covers and to identify where to find documentation on the FortiClient Configurator Tool and the FortiClient Rebranding Tool.
2017-07-20	Updated to clarify support for FortiSandbox 2.4.0 and later and how to bypass the FortiSandbox authorization. See Product Integration and Support on page 14. Also added 0441793 to *Known Issues*.
2017-08-03	Clarified Windows server supports Vulnerability Scan as well as Antivirus.
2017-08-09	Added 0396625 to Resolved Issues and added a special notice about nested VPN tunnels.
2017-11-23	Updated *Special Notices* by adding *Change in SSL VPN default* and updating *Transition to OS Certificate Store instead of FortiClient's local certificate store* to clarify that FortiClient (Windows) supports certificates.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.6.0 build 1075.

- Introduction
- Special Notices
- What's New in FortiClient (Windows) 5.6.0
- Installation Information
- Product Integration and Support
- Resolved Issues
- Known Issues

Please review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone Mode
- Managed Mode

Standalone Mode

In standalone mode, FortiClient is not registered to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free both for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed Mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can register to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient Licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient Licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

Change in SSL VPN default

Starting with FortiClient 5.4.4, TLS is the default used for SSL VPN when establishing a tunnel connection with FortiGate. Previously with FortiClient 5.4.0 to 5.4.3, DTLS was the default. After you upgrade to FortiClient 5.4.4, you can configure DTLS to be the default by setting the following XML element in the FortiClient configuration file: `<prefer_dtls_tunnel>1<prefer_dtls_tunnel>`

When `<prefer_dtls_tunnel>` is set to `0`, FortiClient uses TLS, even if `dtls-tunnel` is enabled on FortiGate.

When `<prefer_dtls_tunnel>` is set to `1`, FortiClient uses DTLS, if it is enabled on the FortiGate and tunnel establishment is successful. If `dtls-tunnel` is disabled on FortiGate, or tunnel establishment is not successful, TLS is used.

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN 98% issues

New SSL VPN Windows Driver has been introduced, which will help resolve various SSL VPN connection issues. The new driver will help increase the performance by up to 20% and provide a stable VPN connection.

Windows notification of AV being disabled

In FortiClient 5.6.0, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopping running.

Transition to OS Certificate Store instead of FortiClient's local certificate store

FortiClient (Windows) supports certificates using OS certificate store. However, FortiClient (Windows) no longer supports the use of FortiClient's own local certificate store, and it is recommended that you use Windows Certificates Store instead. If you are currently using FortiClient's local certificate store, you should transition to Windows Certificates Store before upgrading to FortiClient (Windows) 5.6.0.

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

What's New in FortiClient (Windows) 5.6.0

This section identifies the new features and enhancements in FortiClient (Windows) 5.6.0. For more information, see the *FortiClient Administration Guide*.

FortiClient install option

FortiClient installer now only installs features required for the solution chosen by user at the time of install.

Improved FortiClient compliance feature

FortiClient endpoint compliance is now enforced by FortiOS where administrator can either warn or block non-compliant endpoints. FortiClient dashboard will display the compliance status and reason for non-compliance. FortiClient dashboard will also include information on the configuration settings that is causing non-compliance.

Vulnerability Scan GUI

The FortiClient GUI for the Vulnerability feature has been improved to show details on detected vulnerabilities and patch status and to identify software failed to be auto-patched. The improved display of the results helps improve usability, where the user can easily identify outstanding vulnerabilities that may need to be fixed manually.

User Avatar retrieval from cloud applications

FortiClient can now be used to retrieve username and user avatar from third-party cloud application, such as LinkedIn, Salesforce and Google.

User Avatar sent to FortiAnalyzer

FortiClient can now send user avatar and device information to FortiAnalyzer so that it can be used in FortiView and reports.

Improved remote logging to FortiAnalyzer

FortiClient endpoints now send detailed logs to FortiAnalyzer so that data can be used for FortiView and custom reports.

Sandbox detection

The Sandbox Detection feature can be used to send files to FortiSandbox for analysis without having to install the AntiVirus feature. This feature can use used with other third-party AV products installed on the endpoint.

The Sandbox Detection feature will quarantine any files found to be malicious by FortiSandbox. You can also send the following file types with supported file extensions to FortiSandbox for analysis: web and email downloads as well as files copied from removable USB drives or network drives.

New SSL VPN Windows Driver

New SSL VPN Windows Driver has been introduced, which will help resolve various SSL VPN connection issues. The new driver will help increase the performance by up to 20% and provide a stable VPN connection.

VPN Auto-Reconnect improvement

When FortiClient VPN auto-connect feature is turned on, and VPN connection fails, a permanent pop-up window is displayed to inform the user about the connection failure. FortiClient will keep re-trying to connect VPN in the background, until the user selects an option from the pop-up window.

Configurator and Rebranding Tools

FortiClient Configurator Tool, which is used to create custom installers, will be available for download for free from Fortinet Developer Network site (http://fndn.fortinet.net/). FortiClient Rebranding Tool is available for download with FNDN site license.

For more information, see the *FortiClient Configurator Tool* and *FortiClient Rebranding Tool* documents on the Document Library at http://docs.fortinet.com/forticlient/admin-guides.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

- FortiClientSetup_5.6.xx.xxxx.exe
  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.6.xx.xxxx.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_5.6.xx.xxxx_x64.exe
  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.6.xx.xxxx_x64.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_5.6.xx.xxxx.zip
  A zip package containing miscellaneous tools, including VPN Automation files:

The following tools and files are available in the FortiClientTools_5.6.xx.xxxx.zip file:

- FortiClientVirusCleaner
  A virus cleaner
- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- SSLVPNcmdline
  Command line SSL VPN client
- SupportUtils
  Includes diagnostic, uninstallation, and reinstallation tools
- VPNAutomation
  A VPN automation tool

Please review the following sections prior to installing FortiClient version 5.6.0: Introduction on page 6, Special Notices on page 8, and Product Integration and Support on page 14.

Installation options

When installing FortiClient version 5.6.0, you can choose the setup type that best suits your needs. FortiClient will always install the Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

Upgrading from previous FortiClient versions

FortiClient version 5.6.0 supports upgrade from FortiClient versions 5.2 and later.

Downgrading to previous versions

Downgrading FortiClient version 5.6.0 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 5.6.0 support

The following table lists version 5.6.0 product integration and support information.

FortiClient 5.6.0 support information

Desktop Operating Systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 5.6.0 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 5.6.0 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for FortiClient documentation • Windows Installer MSI installer version 3.0 or later.
FortiAnalyzer	• 5.6.0

FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 1.2.0
FortiManager	• 5.6.0
FortiOS	• 5.6.0 Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • 5.4.0 and later
FortiSandbox	• 2.4.0 and later Enforcement of FortiClient authorization should be disabled on FortiSandbox until the feature becomes available in a future version of FortiClient. To disable authorization, run the FortiSandbox CLI command: `device-authorization -f` • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

FortiClient language support

Language	Graphical User Interface	XML Configuration	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔		

Language	Graphical User Interface	XML Configuration	Documentation
Chinese (Traditional)	✔		
French (France)	✔		
German	✔		
Japanese	✔		
Korean	✔		
Portuguese (Brazil)	✔		
Russian	✔		
Spanish (Spain)	✔		

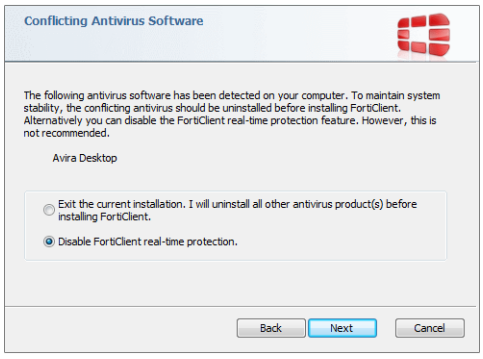
The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 5.6.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
0304447	Auto-connect and Always Up
0377789	Notification Server Gone After FDS or Manual Upgrade
0379372	FortiClient 5.4 causes PC crash on Windows 8.1 Enterprise x64
0380668	When the network connection was up and down, FortiClient does not try to re-connect for SSL VPN
0384558	Send Avatar to FGT and FAZ regardless of the image size
0390067	Unusually high volume of INIT commands (for web filter) from FCT
0390782	XML inconsistent system culture code
0392902	Different OTP challenge window for IPsec and SSL VPN
0393050	Standard user can't upgrade
0394241	FCT broadcast registration on IPsec VPN connection randomly failed
0395069	Fortiproxy keeps restarting
0396879	FCT restores with non-password file still showing password field
0397179	Incorrect *Compliance* tab behavior in the FortiClient GUI when registering to EMS
0398924	Upgrading client should not require admin access rights
0399409	FortiClient 5.4.2 does not install split tunneling routes
0399668	Issues with FortiClient during full scans
0400988	Problem with saved password with certificate-based corporate VPN
0401461	Sec password issues
0401969	Registered and compliance devices still being blocked for a brief time after recovering from sleep mode

Bug ID	Description
0402357	FortiClient upgrade causes "reboot" pop-up loop
0402789	FortiTray IPSec sent and received bytes are switched
0403486	Re-register FCT to FGT fails to work for unregistered FCT
0404824	Application is blocked as Riskware, even when Riskware detection is off
0405113	FortiClient detects EMS server processes as exploit
0405204	SSL exclusive routing doesn't work properly
0405833	HTTP POST request blocked by FortiProxy
0406031	FortiClient Configurator Tool does not apply AV settings from configuration file
0406356	With fresh install of b1016 on Windows 10, message center shows both FCT and windows AV are disabled
0406548	Problem with Numara Track-IT application when WebFilter enabled on FortiClient
0406595	FortiClient CBBS failed to kill running process
0407870	EMS reported wrong VCM engine
0408258	Backup config has `use_legacy_ssl_adapter=1`
0408619	FortiClient 5.6 Beta 1 cannot be installed in Secure Boot environment / A Digitally Signed Driver is Required
0409430	FortiClient dashboard showed wrong lock state when FortiClient was located locally
0410619	Localisation into supported languages
0414854	Folders with commas fail to be added properly when config restored or pushed by EMS to FortiClient
0415065	Remote FAZ logging does not work when using FQDN as remote upload server
0415106	FortiClient should not request new EMS profile after system reboot
0415501	Changing configuration in EMS causes third-party SSL VPN to drop
0416626	FortiClient failed to sync with EMS setting for using Sandbox signature
0416684	Script error when culture code is zh_CN
0416845	SSL VPN -> Bytes sent is not correct

Bug ID	Description
0417061	FortiClient Console crashes when registered to 1.2 EMS
0417286	Diagnostic Tool is missing Windows Update log on Windows 10
0417306	FortiClient 5.4.3 End User Avatar crashes on Windows 7 x86
0421046	*Compliance* tab does not show EMS connection status if "Telemetry" connection is disconnected
0421606	Users cannot log in to SSL VPN site using FortiClient and TokenMobile, when using multibyte for user group name
0422163	Incorrect Compliance Result Flag for Third Party AV Check
0423095	FortiClient shouldn't Install DHCP Server Host Route Entry if SSL VPN Exclusive-Routing Enabled
0423244	Fortiproxy takes high CPU usage with all related features disabled
0423829	With FCT installed, cannot access mail.yahoo.com
0424511	Single Sign On Mobility Agent does not allow multiple FAC server entries

Common Vulnerabilities and Exposures

Bug ID	Description
0396625	FortiClient (Windows) 5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-8493 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in FortiClient (Windows) 5.6.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
0374133	IPsec VPN works with x.509 certificates, but not with Windows certificate store
0378100	FortiClient causes .NET Framework error on Windows 7
0380567	Application Firewall not blocking Micro Applications
0387850	Unable to move FortiClient from old EMS to new EMS
0389865	FortiClient does not check the revocation status of SubCA
0399256	IPsec tunnel before Windows logon - certificate read from Smartcard with PIN failed
0399990	FortiClient v5.4.2 causing BSOD
0400439	FortiSandbox will only Respond to Authorized FortiClient
0403955	FCT VCM scan should exit when there is a scheduled system reboot request
0403955	FortiClient vcm scan should exit when there is scheduled system reboot request
0404746	SSL VPN with certificate auth doesn't work from FortiTray, but works from FortiClient console
0404868	Should pop-up Auto-reconnect failed windows
0405303	Unable to use IPSec VPN with Client/PC PKI Certificate
0409656	FortiClient removed default route of LTE card after connecting to IPsec VPN
0411349	FortiClient prevents WiFi adapter from working after installation
0413851	AV scan stuck on a specific folder
0414476	AV network scan slowing down applications that rely on network resources
0414925	Unable to block www.youtube.com in Firefox
0415789	Unable to connect to SSL VPN if *Do not warn Invalid Server Certificate* is enabled
0415796	EMS deployment of FortiClient results in Installation Error

Bug ID	Description
0416219	FortiShield blocks FortiClient-related applications
0416352	FortiClient doesn't connect to Telemetry Gateway IP after registration
0417707	AV scan history is lost after upgrading FortiClient
0421109	Simplify procedure of changing saved VPN password
0421319	Need to have the option to disable *block malicious websites* when on-net
0421842	Accessing protected network not possible via IPsec Dialup VPN connected using dongle (Airtel) from a Windows 10 computer
0422884	Scan files with AV before sending to the FortiSandbox
0422922	Unable to access landing page
0423673	Unable to use *File Extensions Excluded From Real-time AntiVirus Protection* in FortiClient for OS X
0423685	OpenOffice document (.odt) crashes while browsing when FortiClient 5.4.3 *Real Time Protection* is enabled
0424011	Scheduled reboot not shown
0424102	Fortiproxy Causes Issues with Citrix HTML5
0424218	SSL VPN connection gets stuck with FortiClient 5.6.0.1057
0434078	Quick scan doesn't scan all expected files on some Windows 10
0434095	FortiClient proxy breaking access to Microsoft TFS server
0434174	FCRemove does not delete FortiClient directory
0434207	[VB100] Grayware is not detected in a fresh installation
0434279	`fcaptmon.exe` crash after EMS deployed FCT 5.6.0.1061
0434289	FortiClient b870 with trendmicro AV causes HTTP websites to fail to load on Windows 10
0434355	FortiClient process stayed 100% CPU after registered to FGT
0434485	FortiESNAC crashes on Windows server 2008 R2
0434541	FortiClient scheduler does not start after system reboot

Bug ID	Description
0434551	Cannot enable Sandbox signature detection using restore
0434879	FortiSandbox can't detect files accessed between AP's like Skype
0434983	Fortiproxy process crashed randomly
0434993	Deployment to uninstall FCT, but FCT status doesn't update
0435153	Sandbox stats failed to auto update
0435165	Sandbox still hold files from the trust list source until Sandbox timeout
0435183	VPN before logon, auto initiate a user-defined script upon IPsec/SSL VPN tunnel connection should work
0435209	FCT Sandbox blocked file download from email when enabled Sandbox timeout > 0
0435224	Sandbox exclusion list setting should have high priority over deny file access when sandbox is not reachable
0435799	FortiClient does not send non-unicode user name to FortiSandbox
0435861	`fcdblog process` crashed when trying to shut down FortiClient
0435899	There is no schedule prompt and reboot prompt when upgrading FortiClient 870 to 1068 from EMS
0436001	[Sandbox] Sandbox failed to quarantine malicious file on network drive
0436131	User failed to provide registration IP by clicking Telemetry gateway list
0436238	VCM signature not sent to EMS
0436266	FortiClient log filter failed to work
0436289	IPSec VPN before logon doesn't filter certificate
0436318	FortiClient failed to send FortiClient-specified avatar to FortiAnalyzer
0436719	FortiClient should show avatar after registered
0436725	Non-required features was added after upgrading FortiClient 5.4.3 to FortiClient 5.6.0
0436836	[FSA] User can't open excel file (xlsx) on network drive, if scan for network drive & wait sandbox result are enabled
0436877	FortiClient missed log setting for some features

Bug ID	Description
0437093	Upgrade standalone 5.4.3 FSSO installed full FortiClient
0437125	FortiClient / FortiSandbox integration does not work as expected with Lotus Notes
0437141	FortiClient Telemetry -> wrong next seconds
0437159	Should not remove saved password
0441793	Thunderbird cannot send or receive email (FortiClient App Firewall conflicts with Avast Mail Shield)